There are a number of important pieces of information included. Several main ones might be:

The Information Security and Privacy Conference,
Oct. 17, 2002 at the Sacramento Convention Center
CMS Extension deadline in FAST approaching - Oct. 15
Edits to final privacy regs

As always: Please be sure to note that in some cases the information presented may be the opinion of the original author. We need to be sure to view it in the context of our own organizations and environment. You may need additional information, support, legal opinions and/or decision documentation when interpreting the rules.

My thanks to all the folks who have shared information for this e-news.
Have a great day!!!
Ken

Interesting items below:

Information Security and Privacy Conference - below and see ATTACHMENT
CMS Extension Info
Edits to final privacy regs
HIPAA Implementation Newsletter-- Issue #40 - Friday, August 23, 2002 - ATTACHMENT
[hipaalert] HIPAAlert - lite -- 08/27/02 - ATTACHMENT
Article: HIPAA What States Should Know
[hipaanotes] HIPAAnote - Vol. 2, No. 33 - 08/28/02 - ATTACHMENT
[hipaalive] Security-Privacy Relationship

********* Information Security and Privacy Conference **********
The Information Security and Privacy Conference will be held on October 17, 2002 at the Sacramento Convention Center. This event is in coordination with Art Mark, chair of the Statewide Security Sub-Workgroup for HIPAA. See attachment for details.

Please note that many of the exhibitors are HIPAA-specific.

A possibility, yet to be formally confirmed, is that government staff who include the word "HIPAA" on their registration may be permitted the lowest admission price, and they also will accommodate government staff who are having to deal with no budget - sending an invoice that can be paid after the agency's budget is approved.

When the Privacy track is complete, an updated flyer will be sent out. Note: These presentations will be strictly educational - there will be no selling or marketing.

---- ----------------- ------------- ---------------- ---------------
Many thanks to Bill Roberts and ISSA Bill_Roberts@CalPERS.CA.GOV for extending this conference to include HIPAA topics and issues. Also, many thanks to Art Mark of HHSDC for his work with Bill on this.

Thanks!!!!
Ken

---- ---------- ---------- ---------- ----------

********** CMS Extension Info **********
For Information from CMS related to the Extension Compliance Plan they have a Q&A page at:
http://cmshhs.custhelp.com/cgi-bin/cmshhs.cfg/php/enduser/std_alp.php?p_sid=XMlMEGng&p_lva=333&p_li=&p_gridsort=&p_row_cnt=37&p_search_text=&p_sea
rch_type=3&p_cat_lvl1=2&p_cat_lvl2=25&p_sort_by=dflt&p_page=1

********** edits to final privacy regs **********
Attached is the full document of the privacy regs we emailed previously to you. We have identified some minor edits and wanted to send them to you - the pages where the edits have been done are: 13, 17, 19, 22, 30, and 43. You can remove these pages from any hardcopy you have and then replace them with the edited pages. If you have any questions, please give me a call. Thanks.
<<final privacy regs Aug 02.doc>>
Ruth I. Jacobs, RN
State of California
Health and Human Services Agency
Office of HIPAA Implementation (CalOHI)
1600 Ninth Street, Room 400
Sacramento, CA 95814
(916) 651-6905
Fax: (916) 653-9588
rjacobs1@ohi.ca.gov

********** Article: HIPAA What States Should Know ********
>>> "Huber, Cheri" <CHUBER@co.napa.ca.us> 08/28/02 03:54PM >>>
Here's some more "stuff" for your HIPAA library.

http://www.aphsa.org/wmemohipaa.pdf
<<wmemohipaa.url>>

******** [hipaalive] Security-Privacy Relationship **********
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
I believe it is a big mistake to not incorporate security at this point. The rule sounds very intimidating to people unfamiliar with technology, but to all the network engineers and CISSP's out there it is a laundry list of straightforward practices they've been encouraging for years. The security rule is not final, but if you examine it, you will find that on the whole it is not making huge demands that will be highly changeable (like Privacy's consent provision). The privacy rule covered new ground by pioneering healthcare privacy regulation. The security rule merely mimics what the government has been saying to any industry--their own agencies, e-commerce, banking etc.--regarding a baseline security standard in the network age. The security rule is a best-practices list that summarizes policies and procedures that ANY business should be running, healthcare-related or not.

Let's examine the rule for a second.

There are three main categories of procedures to guard data integrity, confidentiality and availability (funny, the Privacy rule wants to ensure confidentiality and availability as well!)
I have starred the items that I believe should be incorporated with Privacy according to the Minimum Necessary Standard.

1. Administrative procedures
   Certify system security
   Form chain of trust agreements
   Internal auditing*
   Record processing/destruction mechanisms*
   Contingency plans*
   Personnel and system security management*
   Information access control*
   Security awareness training*
   These are almost all a matter of having security responsibility in place. Do you have an IS/IT department? Do you use computers? Do they connect to each other? If so, then you need to make sure that users know how to protect your system. Do you let employees load games on your computers? Can they corrupt critical files to avoid having to work? Can they email medical records to the National Enquirer? Access should be limited. Surely you don't allow everyone in your company to read your email, right? All of these controls are implied by these administrative procedures. The security rule wants you to have a security plan. It doesn't tell you how to do it, just that you need to be as secure as your risks require you to be. If you think that these things don't affect the privacy of information, go to Georgetown's Health Privacy Project website and look at the privacy stories:
http://www.healthprivacy.org/info-url_nocat2302/info-url_nocat_show.htm?doc_id=34777
You'll find that many of them talk about breaches more related to security than anything.

2. Physical safeguards
   Establish security responsibility*
   Media controls*
   Physical access controls*
   Workstation acceptable use policies*
   Security awareness training*
   These cover things such as building security and workstation use. Do you allow anyone to come into every part of your building? Can I come into your building and log on and destroy your network or steal disks containing health information? If not, it's because you have some sort of physical access controls. All that the security rule is demanding is control. Lock your doors, says HIPAA. If you're concerned about people overhearing PHI by the privacy rule and don't care if someone walks into your unlocked medical records vault, something is amiss. Without some sort of security, privacy is meaningless!

3. Technical security services (similar to technical security mechanisms.)
   Automatic log-off*
   Audit trails and alarms (firewall)

Data authentication
Encryption on data transmitted over the internet
Access controls (unique signons, passwords, etc.)*
Virus protection*

This is where you get into portions of the rule that could change as technology changes. Log-offs or locks should be in place to protect the idea of minimum necessary access to PHI. Sounds like the privacy rule. Audit trails and alarms are based on firewall security. You need to know when you have an intruder and how to detect unusual activity patterns. Put something in place to protect yourself. HIPAA doesn't tell you to buy a $500,000 piece of equipment, but it wants a policy and support for that policy. Granted, encryption is problematic because there is no standard across the board. Some vendors might want this type, some might want that, and there is no clear enterprise solution that enables user-friendly encryption both by corporations and home users. I would not take steps as far as encrypting data yet, but I would make efforts to stop emailing PHI in the meantime. Virus protection. Enough said, if you have no virus protection and no user training to support your policy, your system is vulnerable. Everything that you do could disappear with the right type of virus attack, unless you're protected. All HIPAA wants is a basic level of protection. Right now, a hospital could do anything they want, but that will soon change.

In short, without following the security rule to some extent, you will not be adequately following the privacy rule, especially the concept of minimum necessary. With poor security practices you will be very open to complaints and fines. At this point I would not advise spending a lot of money on encryption or the electronic signature standard, but the rest is pretty straightforward and you won't be overdoing it by complying with the general principles espoused by the rule.
Thanks,

Jason Brege